REPUBLIC OF TURKEY
YILDIZ TECHNICAL UNIVERSITY
DEPARTMENT OF COMPUTER ENGINEERING

IDENTITY AUTHENTICATION ON MOBILE DEVICES USING FACE VERIFICATION AND ID IMAGE RECOGNITION

17011907 — Ayşe Hilal DOĞAN
16011016 — Ahmet ELGÜN

SENIOR PROJECT

Advisor
Prof.Dr. Songul VARLI

May, 2021

ACKNOWLEDGEMENTS

Yıldız Technical University is one of the seven government universities situated in İstanbul besides being the 3rd oldest university of Turkey with its history dating back to 1911.It is regarded as one of the best universities in the country as well. Our university has 10 Faculties, 2 Institutes, the Vocational School of Higher Education, the Vocational School for National Palaces and Historical Buildings, the Vocational School for Foreign Languages and more than 25,000 students.

The Istanbul State Engineering and Architectural Academy and affiliated schools of engineering and the related faculties and departments of the Kocaeli State Engineering and Architecture Academy and the Kocaeli Vocational School were merged to form Yıldız University with decree law no.41 dated 20 June 1982 and Law no. 2809 dated 30 March 1982 which accepted the decree law with changes.

The new university incorporated the departments of Science-Literature and Engineering, the Vocational School in Kocaeli, a Science Institute, a Social Sciences Institute and the Foreign Languages, Atatürk Principles and the History of Revolution, Turkish Language, Physical Education and Fine Arts departments affiliated with the Rectorate.

Yıldız Technical University is one of the seven government universities situated in İstanbul besides being the 3rd oldest university of Turkey with its history dating back to 1911.It is regarded as one of the best universities in the country as well.

Ayşe Hilal DOĞAN
Ahmet ELGÜN

TABLE OF CONTENTS

LIST OF SYMBOLS

Ai	Activities of Daily Life
c	Alternate Step Test
C	Body Mass Index
CR	Cross Step moving on Four Stops
$fc(.)$	Dynamic Bayesian Networks
ΔH	Demura's Fall Risk Assessment Chart
λi	Electromyography
Ω	Faculdade de Engenharia da Universidade do Porto

LIST OF ABBREVIATIONS

ID	Identity Card
LFW	Labeled Faces in the Wild
OCR	Optical Character Recognition
RAM	Random Access Memory

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

IDENTITY AUTHENTICATION ON MOBILE DEVICES USING FACE VERIFICATION AND ID IMAGE RECOGNITION

Ayşe Hilal DOĞAN
Ahmet ELGÜN

Department of Computer Engineering
Senior Project

Advisor: Prof.Dr. Songul VARLI

With the changing and developing world, the needs of people are increasing day by day. Technology continues to be the solution to our problems. Especially after the pandemic, the importance of technology has increased even more. Transactions that require authentication have started to be done remotely and are rapidly becoming widespread. Remote banking, notary transactions, tax and land registry transactions, population transactions can be given as examples of transactions that require identity verification.

Although e-signature is generally used for authentication in Republic of Turkey, but e-signature is an expensive method and difficult for everyone to access. As an alternative method to this, authentication with face verification has become widespread and a method has emerged that can make identity verification easier and more reliable in the internet environment.

In this project, a system has been developed to implement the remote authentication method. In this system, ID authentication is done by removing the identity information from the identity photo that the user uploads to the system and the photo of the person on the ID is matched with the photo taken instantly and live, and it is checked whether they are the same person. If all the steps are successful, the authentication is done.

This system is adaptable and usable in systems such as banking and notary public.

Image processing and artificial neural networks are used in this project. MTCNN detector was used for face recognition, VGGFace model was used for face verification, and OCR detector was used for obtaining identity information.

Keywords: e-signature, ID, Image processing, Neural networks, MTCNN, VGGFace, OCR

ÖZET

IDENTITY AUTHENTICATION ON MOBILE DEVICES USING FACE VERIFICATION AND ID IMAGE RECOGNITION

Ayşe Hilal DOĞAN
Ahmet ELGÜN

Bilgisayar Mühendisliği Bölümü
Bitirme Projesi

Danışman: Prof.Dr. Songül VARLI

Değişen ve gelişen dünya ile beraber her geçen gün insanların ihtiyaçları da artmaktadır. Teknoloji, sorunlara çözüm olmaya devam etmektedir. Özellikle pandemi sonrası teknolojinin önemi daha da ön plana çıkmıştır. Kimlik doğrulaması gerektiren işlemler uzaktan yapılmaya başlanmış ve hızla yaygınlaşmaktadır. Uzaktan bankacılık, noterlik işlemleri, vergi ve tapu işlemleri, nüfus işlemleri kimlik doğrulaması gerektiren işlemlere örnek verilebilir.

Kimlik doğrulaması için Türkiye'de genellikle e-imza kullanılsa da, e-imza pahalı bir yöntemdir ve herkesin ulaşımı zordur. Buna alternatif yöntem olarak yüz doğrulaması ile kimlik doğrulaması yapılması yaygınlaşmaya başlamıştır ve internet ortamında kimlik doğrulamasını daha kolay ve güvenilir yapabilecek bir yöntem ortaya çıkmıştır.

Bu projede, uzaktan kimlik doğrulama yöntemini uygulamak için bir sistem geliştirilmiştir. Bu sistemde, kullanıcının sisteme yüklediği kimlik fotoğrafından kimlik bilgileri çıkartılarak kimlik doğrulaması yapılır ve kişinin kimlik üzerinde bulunan fotoğrafı ile anlık ve canlı olarak çekilen fotoğrafı eşleştirilir ve aynı kişi olup olmadığı kontrol edilir. Bütün adımlar başarılı olursa kimlik doğrulaması gerçekleşmiş olur.

Bu sistem bankacılık, noterlik gibi sistemlere uyarlanabilir ve kullanılabilir şekildedir.

Bu projede görüntü işleme ve yapay sinir ağları kullanılmıştır. Yüz tanıma için MTCNN dedektörü, yüz doğrulama için VGGFace modeli, kimlik bilgilerinin alınması için OCR

dedektörü kullanılmıştır.

Anahtar Kelimeler: e-imza, Görüntü işleme, Yapay sinir ağları, MTCNN, VGGFace, OCR

1
Introduction

Digitalism now covers a large area of our lives and consequently, the number of transactions requiring remote identification is increasing. As an example; banking, notary, insurance services can be provided. Insufficient security practices used in these areas result with identity theft.

1.1 What is Multi-Factor Authentication?

Multi-factor authentication can be a successful solution to prevent identity theft. For multi-factor authentication we need to extract the identity information from the identity card photo belongs to the user and verify that the ID card belongs to the user who is making the transaction. Every citizen living in the Republic of Turkey has an identity card with a photograph on it. Here is a sample card example in Figure 1.1 which has a photograph on it.

Figure 1.1 The sample of Turkish citizens ID card

1.2 Project Scope

We designed a service that uses face verification and ID card recognition to perform personal identity authentication automatically. First, the user supposed to create an account by choosing an email and password and entering contact information. After creating an account, user logs in the application with his/her email and password. If

the user logs in successfully, the user supposed to upload a photo of the ID card. The program extracts and verifies data in real time automatically from the ID card. Then the program will take video and extracts a few photos from the video to catch the users face correctly. System will compare the photo on the ID card with the photo taken from camera and gives a result. If all the stages are passed, the identity authentication will be validated in seconds automatically.

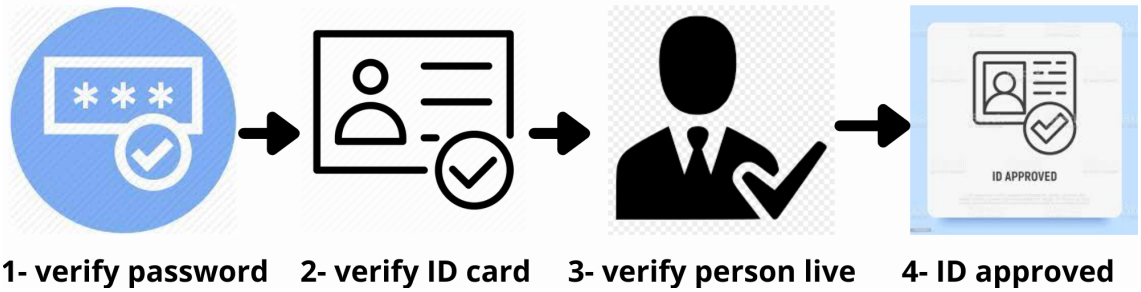

Figure 1.2 Authentication steps

2
Preliminary Examination

Our goal is to create an automatic authentication system that is adaptable to use in different areas. In previous identity verification studies, after the extraction of identity information from ID card, it is checked that the information in the ID matches the information of the person registered in the system or checked if your ID card is fake or checked the similarity between the photo on the identity card with the photo uploaded with his hand-held ID card.

2.1 Related Works

Several existing approaches for the extraction of identity information from ID cards have been proposed. These include text detection, character recognition, and optical character recognition.

The most common approach to extract identity information is to perform text detection and character recognition of the captured image. It involves detecting the text, extracting the characters, and finally recognizing the characters.

The extracted characters are then recognized. Some techniques include the OCR of the characters, the detection of the numerals, and the recognition of the encoding. The optical character recognition technique is to identify the character by its appearance. It can be performed by using the dictionary matching, template matching, or neural network methods. The dictionary matching method uses a pre-trained dictionary.

Face verification, unlike face identification, is known as one-to-one face verification, it serves to verify whether two face images belong to the same person [1]. Face recognition focus on choosing who this person is in the existing dataset. It's also called one-to-many face identification [2]. In the proposed authentication framework, face verification is indispensable. In order to ensure the claimed identity information belongs to the user, it's necessary to verify the faces on the captured ID photo to avoid fraudulent attackers.

2.2 Project Overview

In the web program we have developed for the use of authentication system , the user logs in to the system with the previously determined password and e-mail, upload the identity photo to the system and the system authenticates the ID card. If the authentication is successful, the program will take a photo of the person and find a similarity with the photo extracted from the ID card. Thus, it is checked whether it is the same person.

In the system we developed, the photo is extracted from the ID card and this photo is checked to match the instant photograph of the person in front of the camera and at the same time, it is determined whether the identity is fake or not by extracting information from the ID card.

After extracting information from the identity, using these information, automatic verification is performed for the Republic of Turkey ID cards via E-Devlet (identity verification system) to check whether the identity is fake or not.

To make the face recognition, we developed a Face Recognition model using transfer learning on a pre-trained Deep Learning model VGGFace with ResNet50 architecture and use this new model in the id recognition system that we developed.

VGG-Face is deeper than Facebook's Deep Face, it has 22 layers and 37 deep units. We used CASIA-WebFace data by splitting. CASIA-WebFace is a dataset for training which contains 494,414 face images of 10,575 real identities collected from the web [3].

To make the face verification between the photo extracted from the ID card and the photo of the user, we use cosine similarity function after face recognition method.

We conducted our study by considering the pros and cons of previous researches.

3
Feasibility

3.1 Technical Feasibility

This project is designed in 4 parts. Web application, extraction of credentials, authentication of credentials and face verification.

Python programming language was used for this project. Because the software required for this project can work with Python and both students know Python.

In the web application, the user enters his own information, uploads his ID photo and takes a photo of his face. Since we will be using python for face verification, the web application is also written in Python. Flask library was used with Python.

OpenCV and Tesseract-OCR are used to extract information from identity due to its ease of use, high accuracy and ability to work with Python.

VGGFace model developed for face recognition is used. Because it offers a higher accuracy rate than VGGFace alternatives. Tensorflow is also included in the project to use the VGGFace model.

As the operating system, the Ubuntu operating system was used because both Python and Tensorflow are easy to use and a free operating system.

2GB of RAM and a 1-core processor were found to be sufficient in the server.

Nginx is used as a web server, as it can run high performance on Linux.

3.2 Time Feasibility

The project was divided into parts and shared among the students. Ahmet Elgun made the parts of the web application and the information extraction from the ID card, and the parts of face verification and ID card verification were made by Ayse Hilal Doğan.

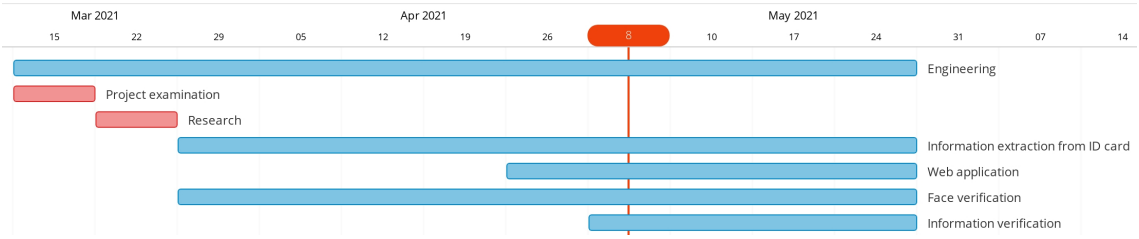

Figure 3.1 Time feasibility

3.3 Legal Feasibility

During the research and realization of the existing regulations and laws related to the project, no patent infringement was made and no pirated software was used.

3.4 Economic Feasibility

Since the necessary equipment for the realization of the project is already in the hands of the project developer, there will be no additional equipment cost. Since all the software used is free and open source software and there are no license fees, there was no software cost.

4
System Analysis

4.1 Challenges

It is important to extract identity information from ID cards because it can be used for a wide range of applications, such as passport authentication, age verification, and fraud detection.

The extraction of identity information from ID cards is a challenging task. Firstly, the text is generally displayed in an irregular font, which makes the recognition task challenging. Secondly, the text is often distorted due to the card being bent, worn out, or damaged. Thirdly, there is no uniform text layout on ID cards, and the text layout depends on the issuing authority and the country where the card is issued.

4.2 Goals

The user can verify his identity after uploading his ID card photo and his own photo to the system. Meanwhile, the system tries to verify the credentials from the authentication service by reading the user information over the ID card. If the information is correct, the picture of the user is tried to be verified with the picture on the identity card. In this study, identity card alone ids not enough for verification. In this way, identity card theft and malicious transactions are prevented.

This project has two important parts. Information extraction from ID card and face matching. OCR technologies should be investigated to extract information from the ID card. Methods used for face recognition should be investigated.

Applications using similar technologies have been studied and tested to find the requirements of this project. Articles similar to our study have been read.

5
System Design

5.1 Software Design

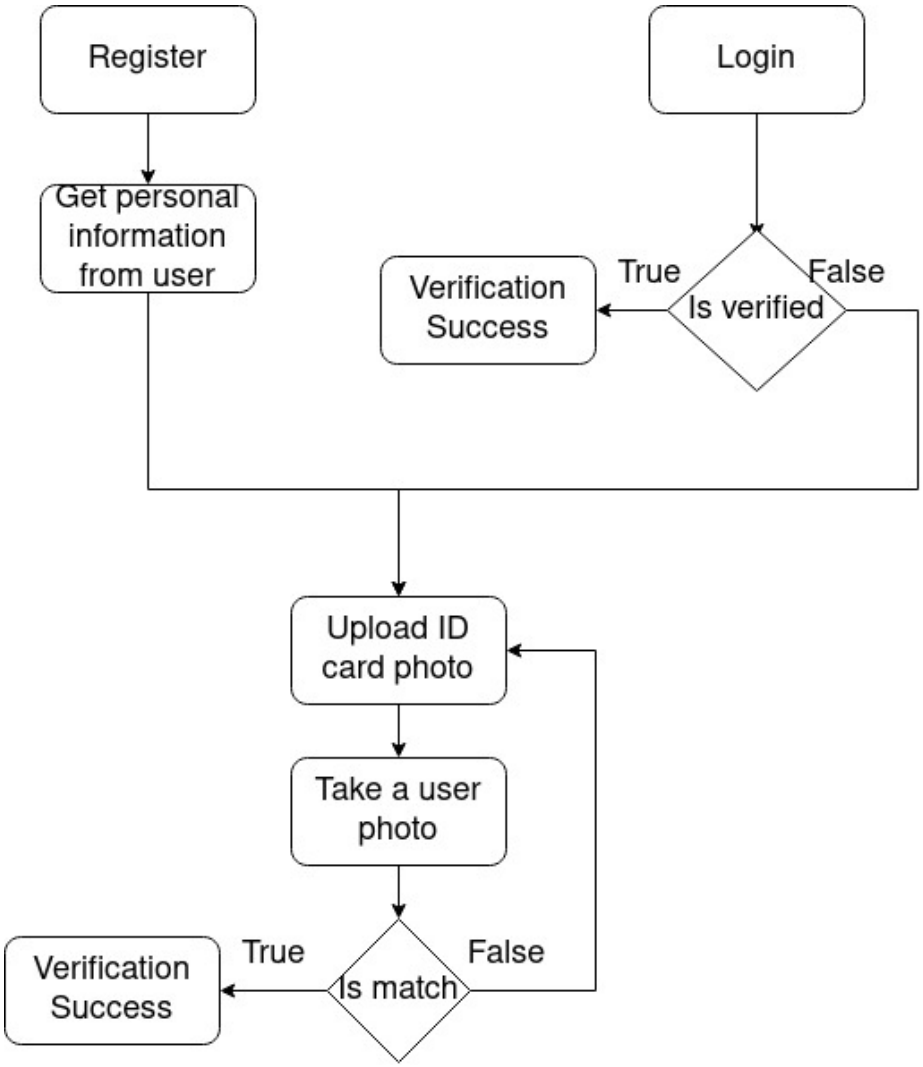

Figure 5.1 Web application design

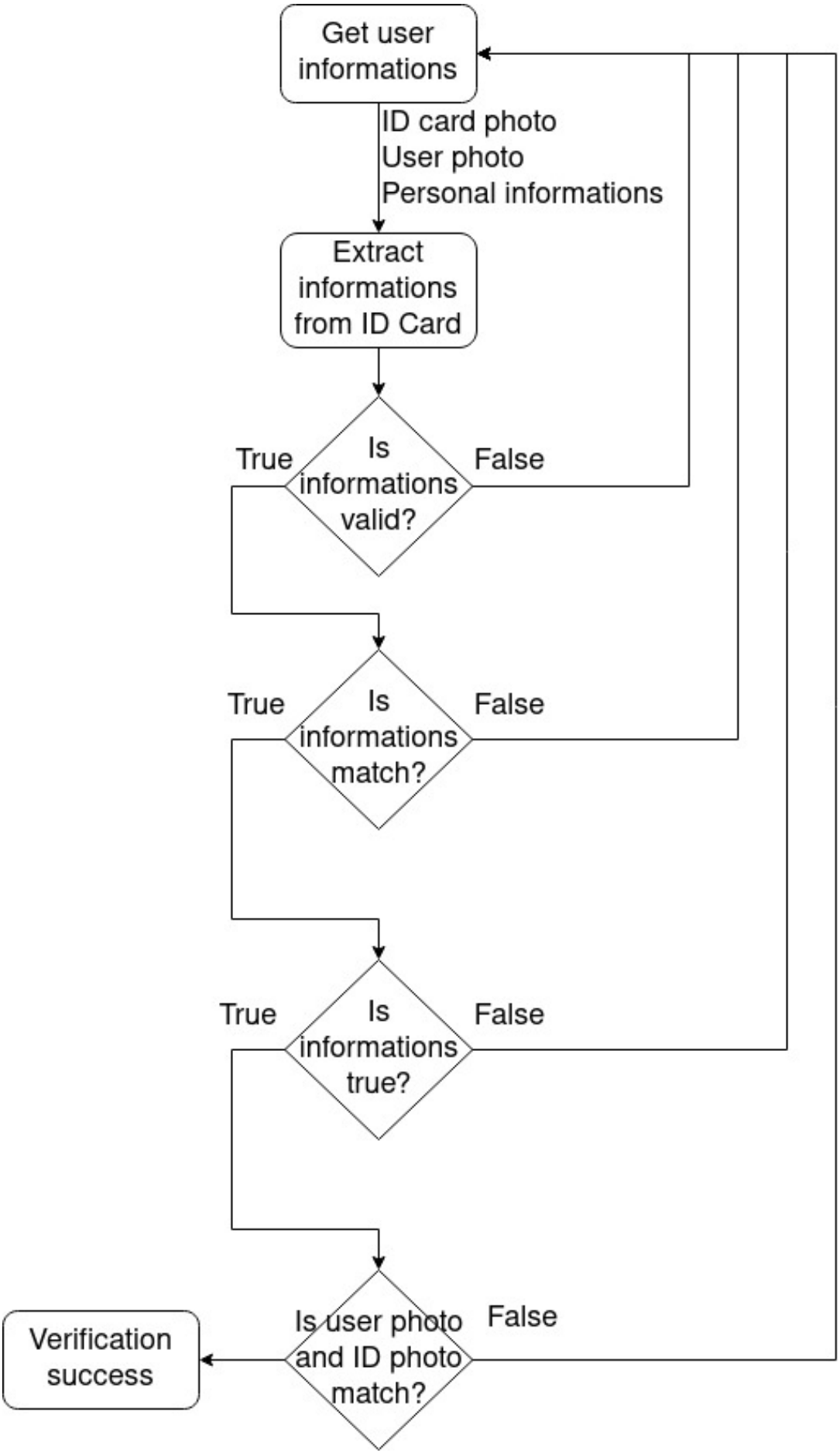

Figure 5.2 Backend Design

5.2 Dataset Design

Two different data sets were used in this study.

5.2.1 LFW Dataset

LFW is a frequently used data set for face recognition. It was prepared in 2007 at the Massachusetts Institute of Technology. These data are generally collected from the internet. It contains a total of more than 13000 face images of more than 5000 people.[4]

5.2.2 CASIA-Webface

This dataset was used for training while Transfer Learning. CASIA-Webface contains more than 500000 photos of more than 10000 people.

6
Application

Here are some example screenshots of the working program.

6.1 Screenshots For Face Authentication

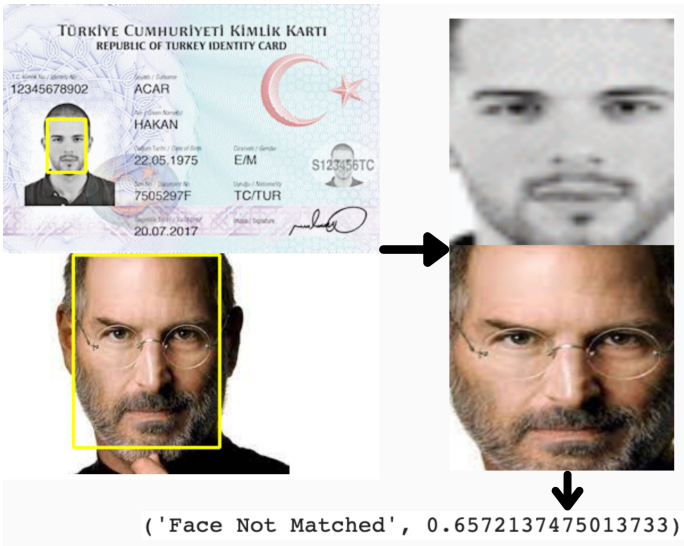

Figure 6.1 Example of match result of 2 different person

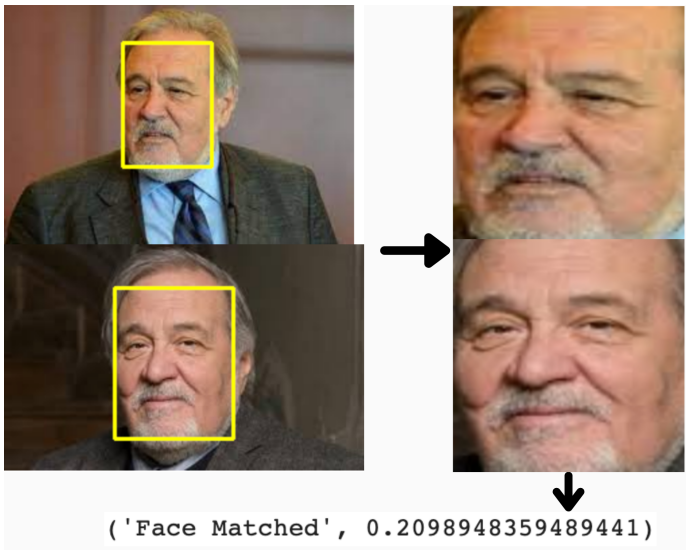

Figure 6.2 Example of match result of the faces belonging to one person

6.2 Screenshots For Information Extraction From ID Card

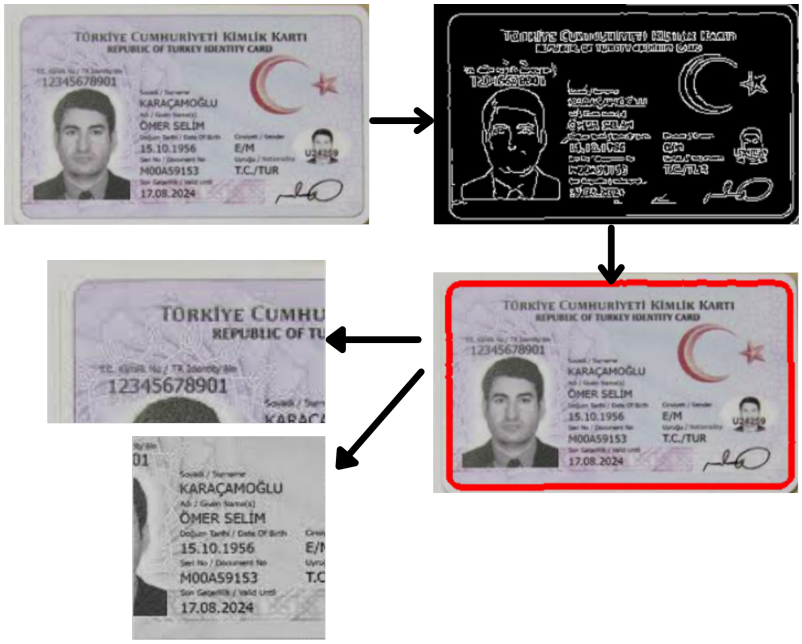

Figure 6.3 Processing of information extraction from ID card


```
tc_data = pytesseract.image_to_string(TC)
tc_no = re.findall(r"[0-9]{11}",tc_data)[0]
tc_no
```

```
12345678901
```

Figure 6.4 Information extraction from ID card taking the id number


```
name_data = pytesseract.image_to_string(NAME, lang="tur")
surname = re.findall(surname_regex, name_data)[0]
firstname = re.findall(name_regex, name_data)[0]
birth_date = re.findall(date_regex, name_data)[0]
valid_until = re.findall(date_regex, name_data)[1]
document_no = re.findall(document_no_regex, name_data)[0]
```

```
print(f"surname: {surname}")
print(f"name: {firstname}")
print(f"birth_date: {birth_date}")
print(f"valid_until: {valid_until}")
print(f"document_no: {document_no}")
```

```
surname: KARAÇAMOĞLU
name: ÖMER SELİM
birth_date: 15.10.1956
valid_until: 17.08.2024
document_no: M00A59153
```

Figure 6.5 Information extraction from ID card taking informations

6.3 Screenshots For Model Summary

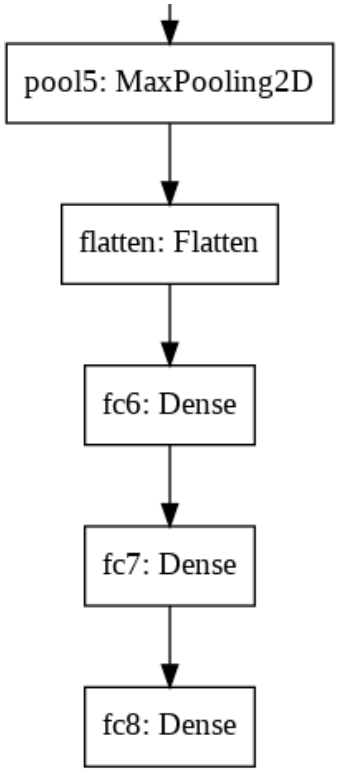

Figure 6.6 Model layers after training

```
_________________________________________________________________
pool3 (MaxPooling2D)         (None, 28, 28, 256)       0
_________________________________________________________________
conv4_1 (Conv2D)             (None, 28, 28, 512)       1180160
_________________________________________________________________
conv4_2 (Conv2D)             (None, 28, 28, 512)       2359808
_________________________________________________________________
conv4_3 (Conv2D)             (None, 28, 28, 512)       2359808
_________________________________________________________________
pool4 (MaxPooling2D)         (None, 14, 14, 512)       0
_________________________________________________________________
conv5_1 (Conv2D)             (None, 14, 14, 512)       2359808
_________________________________________________________________
conv5_2 (Conv2D)             (None, 14, 14, 512)       2359808
_________________________________________________________________
conv5_3 (Conv2D)             (None, 14, 14, 512)       2359808
_________________________________________________________________
pool5 (MaxPooling2D)         (None, 7, 7, 512)         0
_________________________________________________________________
flatten (Flatten)            (None, 25088)             0
_________________________________________________________________
fc6 (Dense)                  (None, 512)               12845568
_________________________________________________________________
fc7 (Dense)                  (None, 512)               262656
_________________________________________________________________
fc8 (Dense)                  (None, 100)               51300
=================================================================
Total params: 27,874,212
Trainable params: 13,159,524
Non-trainable params: 14,714,688
```

Figure 6.7 Model summary

7
Experimantal Results

7.1 Edge Cases

7.1.1 ID Card Cases

It is expected that the photo of the ID card given to the system should be taken straight. Photos taken sideways or upside down cannot be recognized.

The Republic of Turkey Identity Card was used in this project. Other country ID cards, passports and driver's licenses are not valid.

If the ID card photo is blurry, the resolution is low, or the photo is too dark or too bright, the ID card will be difficult to recognize.

Figure 7.1 Recognizable ID Card / Unrecognizable ID Card

If the ID card is taken on light backgrounds, it becomes difficult to distinguish the ID card. This is because the identity card is also light-colored, making it difficult to distinguish the edges of the identity card. Likewise, it becomes difficult to distinguish the identity card on backgrounds with many geometric shapes.

7.1.2 User Photograph Cases

If the user photo does not have a human face, the user cannot be authenticated. As mentioned above, the face may not be detected if the photo is blurry, of poor quality, or is too bright or too dark.

If there is more than one person in the photo, the system will return a negative result because the system cannot know which face to take. Differences such as hair, beard, glasses, hat, make-up may also cause the system to give incorrect results.

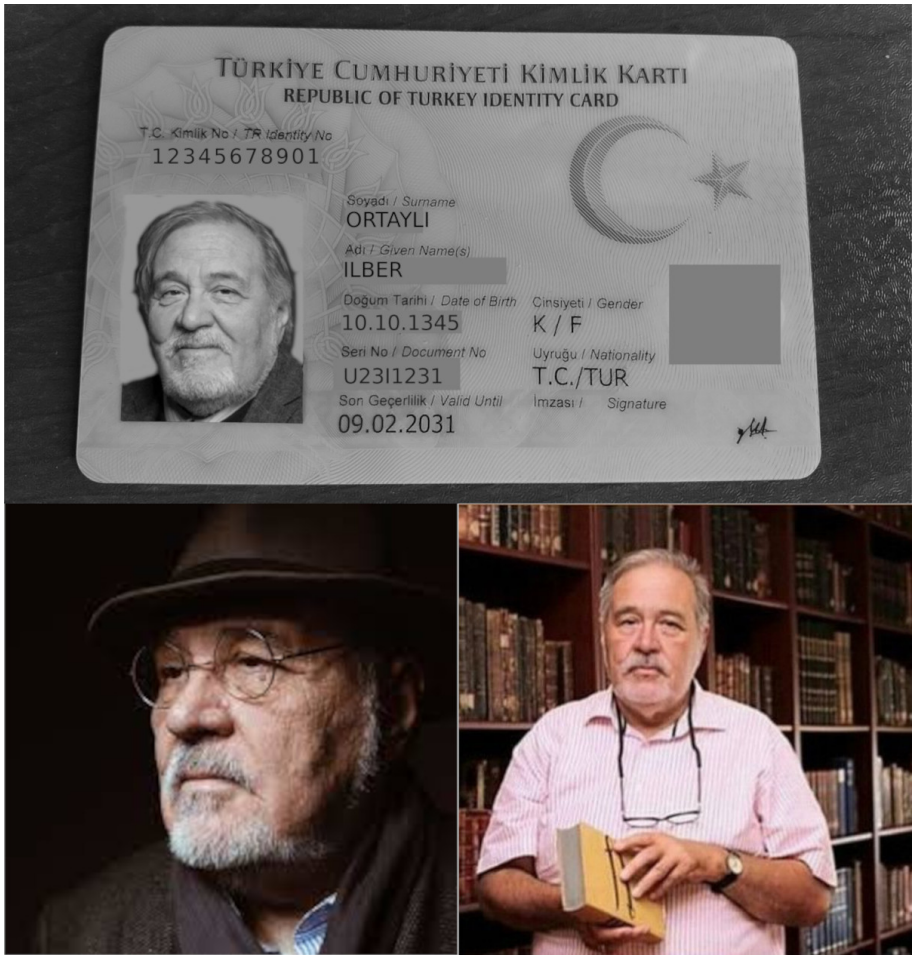

Figure 7.2 Example ID Card and unmatched photo (left) and matched photo (right)

8
Performance Analysis

8.1 Performance Analysis of the Face Authentication

In this project, during the development of the face verification system, training was conducted on pre-trained models using the CASIA-WebFace dataset.

In this study, different experiments were carried out in order to compare the performance of the models.

In the first model a; flatten and dense layers were added on the pre-trained vgg16 (with resnet-50 architecture) model. We did the last layer trainable and there were 5,346,841 trainable values in the model after adding the layers. For this model, we split the CASIA-WebFace dataset and took 25 classes of it to train and test the model. We split it like 80 train, 10 validation, 10 test data. The accuracy was 0.70 after training 10 epoch.

In the second model b; flatten and dense layers were added on the pre-trained vgg16 (with resnet-50 architecture) model just like the a model. We did the last four layers trainable and there were 7,288,516 trainable values in the model. We use the 25 classes of the dataset like first model to train and test. We split it like 80 train, 10 validation, 10 test data. The accuracy was 0.73 after training 10 epoch.

In the third model c; flatten layer, 2 dense(512) layer, 1 dense(256) layer were added on the pre-trained VGGFace model. There were 13,239,552 trainable values in the model after adding the layers. For this model, we split the CASIA-WebFace dataset and took 100 classes of it to train and test the model. We split it like 80 train, 10 validation, 10 test data. The accuracy was 0.82 after training 20 epochs.

In the last model d; flatten layer, 2 dense(512) layer, 1 dense(256) layer were added on the pre-trained VGGFace model just like the c model.But this time we trained the model on 256 classes taken from CASIA-WebFace. We split it like 80 train, 10 validation, 10 test data. The accuracy was 0.83 after training 20 epochs.

If we look at the models that we have trained, we can say that the most successful model is the last one (d model). When we compare the first two models, we can say that if there is more trainable values, the accuracy increase because the other conditions are the same for the model a and b. When we look at the c and d models, d model gives slightly better results because that the class number is more than the c model.

The comparisons of the models is below.

Table 8.1 Trained Models

Model	Pretrained Model	Number of Classes	Layers	Trainable Values	Accuracy
a	VGG16(resnet50)	25	Flatten Dense(25)	5,346,841	0.70
b	VGG16(resnet50)	25	Flatten Dense(25)	7,288,516	0.73
c	VGGFace	100	Flatten Dense(512) Dense(512) Dense(100)	13,239,552	0.82
d	VGGFace	256	Flatten Dense(512) Dense(512) Dense(256)	13,239,552	0.83

8.2 Performance Analysis of the Identity Authentication

The other part of the project is, taking the identification information from the Identity Card. We used OCR to perform this. It is successful but sometimes it may have trouble taking the turkish letters if the ID card photo is blurry, dark or too bright (Figure 7.1). Because the ID card will be difficult to recognize. Example, it can see 'ş' as a 's' or 'ğ' as a 'g'. But the system ignores it and does not cause problems.

References

[1] F. Schroff, D. Kalenichenko, and J. Philbin, "Facenet: A unified embedding for face recognition and clustering," *2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, Jun. 2015. DOI: 10.1109/cvpr.2015.7298682. [Online]. Available: http://dx.doi.org/10.1109/CVPR.2015.7298682.

[2] W. Hu, Y. Huang, F. Zhang, R. Li, W. Li, and G. Yuan, *Seqface: Make full use of sequence information for face recognition*, 2018. arXiv: 1803.06524 [cs.CV].

[3] D. Yi, Z. Lei, S. Liao, and S. Z. Li, *Learning face representation from scratch*, 2014. arXiv: 1411.7923 [cs.CV].

[4] G. B. Huang, M. Ramesh, T. Berg, and E. Learned-Miller, "Labeled faces in the wild: A database for studying face recognition in unconstrained environments," University of Massachusetts, Amherst, Tech. Rep. 07-49, Oct. 2007.

Curriculum Vitae

FIRST MEMBER

Name-Surname: Ayşe Hilal DOĞAN
Birthdate and Place of Birth: 20.12.1998, Florida/ABD
E-mail: l1117907@std.yildiz.edu.tr
Phone: 0531 553 33 45
Practical Training: Codevist Teknoloji A.Ş.
Tübitak Bilgem

SECOND MEMBER

Name-Surname: Ahmet ELGÜN
Birthdate and Place of Birth: 23.09.1998, Denizli
E-mail: l1116016@std.yildiz.edu.tr
Phone: 0534 569 08 36
Practical Training: Smart Pulse Teknoloji A.Ş.

Project System Informations

System and Software: Ubuntu, Python
Required RAM: 2GB
Required Disk: 8GB